

ADDRESS BOOK BUILDER FOR NETWORK MONITORING

NORLINA BINTI PARAMAN

**A dissertation submitted in partial fulfilment of the requirements
for the award of the degree of Master of
Engineering (Electrical-Electronics & Telecommunication)**

**Faculty of Electrical Engineering
University Technology Malaysia**

NOVEMBER, 2005

Specially dedicated to my family, mum and dad for their support and eternal love. To all my friends especially Amin, Yanti, Eni, Sue, Nansah, Atim, Mida, Tini and Zatul thanks a lot for your helping. And for my beloved once, Faizal thanks for being understanding person to me.

ACKNOWLEDGEMENTS

Praise to Allah, the Most Gracious and Most Merciful, Who has created the mankind with knowledge, wisdom and power. First of all, the author would like to express his deepest gratitude to Associate. Professor Muhammad Mun'im Bin Ahmad Zabidi for his continuous support, supervision and encouragement during the course of this project. The author would not have completed this project successfully without his assistance. The author is thankful to all friends for their advice and helpful cooperation during the period of this project. Appreciation is also acknowledged to those who have contributed directly or indirectly in the completion of this project. The author would also like to extend his appreciation to his family members, for their support, patience and endless love.

ABSTRACT

Software development for network monitoring is very important to discover new ways of attacking computer networks. The Network Address Book Builder is the software that is aimed at assisting network administrators in their daily work. PHP and Python were the programming languages used. MYSQL (Standard Query Language) database and Tethereal were used to build software that will be running in FKE campus. It currently runs only on Linux operating system. The methodology to gain output includes a few procedures. The software will capture packets when a user logs into the FKE staff portal to check email. A Python script running as a daemon, analyses the packets to produce output like usernames, MAC (Media Access Protocol) addresses and IP (Internet Protocol) addresses. MAC address and IP address will be matched automatically on the MySQL database table according to the staff username which are in the database. To find the owner of the packets, administrator need to click MAC Address button on the PHP admin graphic user interface (GUI). Besides, the administrator can also search through the MySQL command line.

ABSTRAK

Pembangunan perisian untuk kawalan rangkaian adalah sangat penting untuk mengatasi serangan terhadap rangkaian komputer. Perisian *Network Address Book Builder* adalah sebuah perisian yang bertujuan untuk membantu pentadbir rangkaian di dalam kerja harian mereka. Metodologi untuk mendapatkan keluaran melibatkan beberapa kaedah. Bahasa *PHP* dan *Python*, pangkalan data *MYSQL (Standard Query Language)* dan *Tethereal* digunakan untuk membina perisian yang beroperasi di kampus FKE sahaja pada sistem pengoperasian *Linux*. Perisian akan mempunyai *packet* apabila pengguna mendaftar di FKE kakitangan portal untuk menyemak email. Skrip *Python* menganalisa *packet* tersebut untuk menghasilkan keluaran seperti *username*, *MAC (Media Acces Protocol) address* dan *IP (Internet Protocol) address*. *MAC address* dan *IP address* akan dimasukkan secara langsung ke dalam *MYSQL* pangkalan data berpandukan kepada kakitangan *username* yang sudah ada di dalam pangkalan data. Untuk mencari siapa pemilik *packet*, pentadbir perlu memasuki butang *MAC address* di antaramuka grafik *PHP admin*. Selain daripada itu, pentadbir boleh mencari menggunakan *MYSQL command line*.

LIST OF CONTENTS

CHAPTER	CONTENT	PAGE
	DECLARATION	ii
	DEDICATION	iii
	ACKNOWLEDGEMENTS	iv
	ABSTRACT	v
	ABSTRAK	vi
	LIST OF CONTENTS	vii
	LIST OF TABLES	xi
	LIST OF FIGURES	xii
	LIST OF ABBREVIATIONS	xiv
	LIST OF APPENDICES	xv
CHAPTER 1	INTRODUCTION	
	1.1 Introduction	1
	1.2 Problem Statements	2
	1.3 Project Objective	2
	1.4 Scope of Project	2

CHAPTER 11	LITERATURE REVIEW	
2.1	Project Background	3
2.2	Network packet Introduction	4
2.3	TCP/IP Protocol	
2.3.1	TCP	6
2.3.2	IP	7
	2.3.2.1 IP Packet Format	8
	2.3.2.2 IP Address Format	10
2.4	PDML Format (XML)	10
	2.4.1 Structure of PDML Document	11
2.5	Previous Work	12
	2.5.1 iNetmon by USM	12
	2.5.1.2 Solution of iNetmon	13
	2.5.1.2.1 iNetmon Portable	13
	2.5.1.2.2 iNetmon Remote	14
	Network Monitoring	
	2.5.1.3 iNetmon Architecture	15
	2.5.1.3.1 Network Statistics	15
	2.5.1.3.2 Network Analyzer	16
	2.5.1.3.3 Network Address	16
	Book	
	2.5.2 UniMon	17
	2.5.2.1 Protocol Analysis	18
	2.5.2.1.1 Info-packet	18
	2.5.2.1.2 Status-packet	19
2.6	Packet Traffic Analyzer	20
	2.6.1 Ethereal	20
	2.6.1.1 Features	21
	2.6.2 Tcpdump	22
	2.6.3 Snort	24

CHAPTER 111 METHODOLOGY

3.1	Architecture of the Software	25
3.1.1	Protocol Graph	25
3.1.2	System Design of Software	26
3.2	Operation of Process	27
3.2.1	Running Python File Script	28
3.2.2	Display Captured Packet in PDML Format (XML)	30
3.2.3	Getting Outputs from Python	32
3.2.4	Database	32
3.2.5	Output	35
3.3	Process Block Diagram	36

CHAPTER 1V RESULTS

4.1	Introduction	37
4.2	Displays Data to Process at Command Line	38
4.3	A Part of Captured Packet in PDML Format	39
4.3.1	Discussion	42
4.4	Outputs List Up into Database	43
4.4.1	Find Owner of the Packet Using MYSQL Command Line	43
4.4.2	Find Owner of the Packet Using GUI of PHP admin	44
4.4.3	Discussion	45
4.3	List all MAC addresses and IP addresses	46
4.3.1	Discussion	47

CHAPTER V CONCLUSION AND SUGGESTION

5.0	Conclusion	47
5.1	Future Works	48

REFERENCES	49
-------------------	----

APPENDIX

Appendix A	51-74
------------	-------

LIST OF TABLES

TABLE	TITLE	PAGE
3.1	Tables in Database Sniffer	33
3.2	Fields in Table Login	33
3.3	Fields in Table Staff	34
3.4	Fields in Table Dump	34

LIST OF FIGURES

FIGURE	TITLE	PAGE
Figure 2.1	TCP/IP Layer	5
Figure 2.2	Encapsulation TCP/IP	6
Figure 2.3	Fourteen Fields Comprise an IP packet.	8
Figure 2.4	An IP Address Consists of 32 Bits, Grouped Into Four Octets	10
Figure 2.5	An Example of PDML Document	11
Figure 3.1	Protocol Graph	26
Figure 3.2	System Design of Software	27
Figure 3.3	GUI of user log in	28
Figure 3.4	Coding to Find Username	29
Figure 3.5	Coding to Find MAC Addresses and IP Addresses	30
Figure 3.6	Coding Setting to PDML	31
Figure 3.7	Example of Packet in PDML	31
Figure 3.8	PHP GUI Search Form	35
Figure 3.9	Database that Have Owner of the Packet	36
Figure 3.10	Process Block Diagram	36
Figure 4.1	Username and Password	39
Figure 4.2	The Time and Date Were Captured	40
Figure 4.3	Position of MAC Address	40
Figure 4.4	Position of IP Address	41

Figure 4.5	Trace Port Number	42
Figure 4.6	Python file script is running at command line	43
Figure 4.7	MYSQL Command Line to See the Username	44
Figure 4.8	GUI of PHP admin	44
Figure 4.9	After matching by username, staff table and login table are combined	45
Figure 4.10	PDML Format displays MAC address and IP address	46
Figure 4.11	MAC address and IP address list up into database automatically	47

LIST OF ABBREVIATIONS

PHP	Programming Hypertext Preprocessor
MYSQL	My Structured Query Language
HTTP	Hyper Text Transfer Protocol
TCP	Transport Control Protocol
IP	Internet Protocol
LAN	Local Area Network
FTP	File Transfer Protocol
UDP	User Datagram Protocol
PDML	Packet Details Markup Language
XML	Extensible Markup Language
NetPDL	Network Protocols Description Language
USM	University Science Malaysia
ASCII	Amsterdam Subversive Center for Information Interchange
ARP	Address Resolution Protocol
NetBIOS	Network Basic Input/Output System
WLAN	Wireless Local Area Network
IPv6	Internet Protocol version 6
ISO/OSI	International Standards Organization/Open Systems Interconnect
IDS	Intrusion Detection System
CGI	Common Gateway Interface
SMB	Server Message Block
GUI	Graphic User Interface

LIST OF APPENDIX

APPENDIX	TITLE	PAGE
A	A PART OF XML PACKET	51-74

CHAPTER I

INTRODUCTION

1.1 Introduction

Computer networks are the backbone and are a critical part of almost every organization. Computer networks facilitate information sharing that requires an efficient, high performance and errorless computer network. Impacts of an inefficient network impacts are unable to protect a network from viruses and intruders, e-mails cannot be received or sent, printers cannot be shared, unable to transfer data and remote database connections would be costly.

When the network is congested, a need to build software that performs data collection and analyses the data to identify problem continuously. Network monitoring is used the methodology used when trying to troubleshoot network related issues, watching network equipment and providing performance analysis.

1.2 Problem Statements

To design software that is able to monitor what is happening on the network in addition to knowing a real owner and a activity list of the owner automatically. All this using software which works by analysing the packets which are passing through it.

1.3 Project Objective

The objective of this project is to build software that will be used to identify owner of the captured packet and a list of its activities. Another objective is to analyse network packet in detail and extract characteristic of the packet.

1.4 Scope Of Project

In this project, the software uses Linux operating system as a platform. For language, Python and PHP were used and MySQL as the database. Ethereal is the main component behind this as it is being used to capture and provide packet data in a human readable and parse-able form. The software is currently running in campus FKE only.

REFERENCES

- [1] Sureswaran, R. (2001). "Network Monitor." In Proceedings of Asia Pacific Advanced Network Conference. 40-44.
- [2] Alberto Leon-Garcia. and Indra Widjaja. (2000). "Communication Networks." McGraw-Hill.
- [3] Hasegawa, T. Kato, T. Yoshiizumi, K. Miki, T. Hokamara, K. and Sawada, K. (1998). "Protocol architecture of high speed TCP/IP service over international ATM network." ATM Workshop Proceedings. 159 – 168.
- [4] Akinlar, C. Udaya Shankar, A. Mukherjee, S. and Braun, D. (2002). "IP Address Configuration Algorithms For Routerless And Single-Router Zeroconf Network ." Computers and Communications Proceedings Seventh International Symposium. 37 – 42.
- [5] Priscilla Dielenberg. (2004). " USM Develops Network Monitoring Tool." <http://www.inetmon.com/netmon5.html>.
- [6] Erhard W, Gutzmann M.M and Libati H.M. (2000). "Network Traffic Analysis and Security Monitoring with UniMon." Proceedings of the IEEE Conference. 439 – 446.
- [7] Richard Sharpe, Ed Warnicke, and Ulf Lamping. (2004). "Ethereal User's Guide V2.00 for Ethereal 0.10.5."
- [8] James Kretcmar. (2004). "Tcpdump: An Open Source Tool for Analyzing Packets." <http://informit.com/articles/article.asp>.
- [9] Trevon Warren. "Intrusion Detection System Part 3. Snort." <http://www.freeos.com/articles/3496/>.

- [10] Caulkins, B.D. Joohan Lee. and Wang, M. (2005) “ Packet- vs. Session-Based Modeling for Intrusion Detection Systems.” 116 – 121.
- [11] Wesley J.Chun. (2001). “Core Python Programming.” Prentice Hall PTR.
- [12] Martin C. Brown. (2000). “Python Annotated Archives.” McGraw-Hill.
- [13] MySQL® Database Server The Foundation of MySQL Network.
<http://www.mysql.com/products/mysql/>